ZIMPERIUM

Ensuring Compliance with RMIT Malaysia Regulation with Zimperium

Secure Mobile Banking in the Digital Age

The Reserve Bank of Malaysia updated this regulation in November 2025 to further strengthen financial institutions' management of technology and cyber risks, improve service availability and resilience of financial services, and maintain public trust in the security of the financial system.

These risks, stemming from potential IT system failures or breaches, pose threats of financial loss, operational disruption, and reputational damage. As financial services increasingly rely on technology, banks must enhance their technology resilience to ensure uninterrupted service and protect customer data. This becomes more critical with the rise of sophisticated cyber threats. Effective management of technology risks, especially in larger and more complex institutions, is essential not only for individual banks but also to safeguard the interconnected financial network, thereby preserving overall confidence in the financial system.

Zimperium's App Security Capabilities Help You Comply

The Mobile Application Protection Suite (MAPS) from Zimperium provides four capabilities, including Mobile Application Security Testing (MAST), App Shielding, Key Protection, and Runtime Protection (RASP). The suite provides mobile app teams with centralized threat visibility and comprehensive in-app protection from development through runtime. It combines both inside-out and outside-in security approaches to help organizations build compliant, secure, and resilient mobile apps.

Here is how MAPS capabilities map to RMIT standards and guidelines:

#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
Section 12: Digital Services					
12.3	The complex and fast evolving digital fraud requires financial institutions to be vigilant against new fraud techniques and proactive in strengthening their cyber defence for customer protection.		✓		
12.3(a)	12.3(a) expand the scope of identification of cybersecurity threats and countermeasures to include customers' mobile devices and access points;		✓		
12.3(b)	adopt layered (defense-in-depth) security controls to protect the digital service application deployed to customers' mobile devices and the relevant banking data contained in it;		✓	✓	✓
12.3(b)	perform continuous surveillance and monitoring to detect any exploitation of the digital service application deployed to customers' mobile devices and ensure the swift upgrade of security controls to mitigate new vulnerabilities;		✓		
12.3(e)	formalise operational arrangement to enable swift		✓		

#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
Section 12: Digital Services					
	coordinated response and rapid upgrade of countermeasures to defend against advanced fraud tactics if a financial institution relies on multiple business functions;				
12.3(f)	conduct regular review by senior management to ensure the effectiveness of digital fraud management and define threshold for escalation of countermeasures considering the actual impact to victims of digital fraud and emerging fraud environment; and		✓		
12.4	A financial institution must ensure that its fraud detection capabilities and rules are updated in a timely manner upon detection of new fraud modus operandi in order to prevent fraudulent transactions or account takeover using stolen customer credentials. This must be supported by appropriate risk analytics to improve the accuracy of fraud detection, that includes continuous upgrade of fraud detection capabilities as specified in Appendix 11 on Fraud Detection Standards.		✓		

#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
Section 12: Digital Services					
Cyber Risk Management					
11.9	A financial institution must conduct annual intelligence-led penetration tests on its internal and external network infrastructure as well as critical systems including web, **mobile** and all external-facing applications.	✓			
11.16	A financial institution must implement appropriate policies for the removal of data on technology equipment, mobile devices or storage media to prevent unauthorized access to data.		✓		
System Development and Acquisition					
10.15	Where a third party software is used, a financial institution should consider the potential risks and impacts a cyber supply chain incident may pose to its overall business operations and services. (a)& (b) included.	✓			

#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
Section 12: Digital Services					
Patch and End-of-Life System Management					
10.17	A financial institution must ensure that all systems including digital services are not running with known security vulnerabilities20, on outdated platform or end-of-life (EOL) technology systems.				
14.6	A financial institution must ensure that the independent external party providing the assurance is competent and has a good track record. The assurance shall address the matters covered in, and comply with, Appendix 9. **Appendix 9 Supervisory Expectations on External Party Assurance** **PART B** - Minimum controls to be assessed by the independent External Service Provider, where applicable.	✓	✓	✓	✓
Appendix 4: Control Measures for Mobile Applications and Devices					
1	A financial institution that offers digital services must be aware	✓	✓	✓	

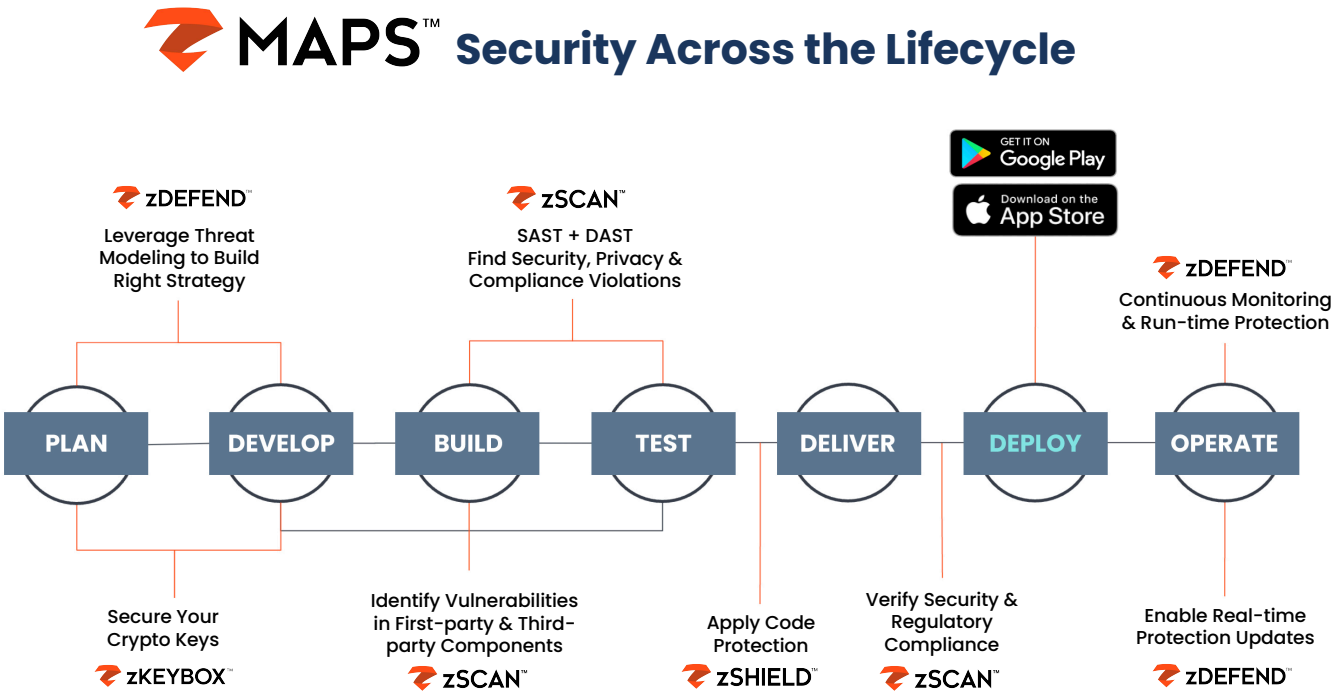
#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
Section 12: Digital Services					
	of the risks associated with mobile applications. To mitigate these risks, a financial institution shall continuously assess and perform risk assessment to ensure that the threats associated with mobile applications is addressed.				
2	A financial institution must ensure digital services involving sensitive customer and counterparty information offered via mobile devices are adequately secured. This includes the following:				
2a	design the mobile application to operate in a secure and tamper-proof environment within the mobile devices to protect users against cyber threats such as malware and unauthorised access;		✓	✓	
2b	prohibit mobile applications from storing customer and counterparty information used for authentication with the application server such as PIN and passwords. Authentication and verification of unique key and PIN must be centralised at the host;	✓			

#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
Section 12: Digital Services					
2c	activation of the mobile application must be subject to robust authentication by the financial institution;				✓
2d	ensure secure provisioning and deprovisioning process of mobile application in the customer's device;				✓
2e	undertake proper due diligence processes to ensure the application distribution platforms used to distribute the mobile application are reputable;		✓		
2f	ensure proper controls are in place to access, maintain and upload the mobile application on application distribution platforms; and		✓		
2g	monitor the application distribution platforms to identify and address the distribution of fake applications in a timely manner.		✓	✓	

#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
Section 12: Digital Services					
3	A financial institution must also ensure the following measures are applied specifically for applications running on mobile devices used by the financial institution, appointed agents or intermediaries for the purpose of processing customer and counterparty information: (a) mobile device to be adequately hardened and secured;		✓	✓	
Appendix 11 - Fraud Standards					
1	A financial institution must establish detailed and comprehensive risk profiles for each customer as a reference point when performing fraud detection based on behavioural analysis of the financial institution's customer and fraud profiles. Examples of relevant factors to be considered may include: (d) behavioural patterns e.g. time taken to make transfer, typing speed, mouse hovering pattern.		✓		

#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
Section 12: Digital Services					
3	A financial institution must implement measures to promptly detect and terminate hijacked sessions to prevent unauthorised access to customer accounts. The financial institution shall notify customer on elevated cyber risk caused by the presence of risky application (e.g. application downloaded outside official distribution platforms or detected to contain security vulnerabilities).		✓		
7	A financial institution must continuously update its system to ensure fraud detection rules remain effective to combat new fraud modus operandi via the following: (a) enhance its fraud detection rules promptly upon detection of new fraud techniques that have evaded its fraud detection system. The enhancements shall be timely upon being notified by its internal fraud team or upon receiving such intelligence from external sources such as other financial institution,		✓		

#	Requirement Description	App Security Testing zSCAN™	Runtime Protection zDEFEND™	App Shielding zSHIELD™	Key Protection zKEYBOX™
Section 12: Digital Services					
	industry group, public-private partnership and other intelligence sharing platform; and (b) review the effectiveness of its fraud detection parameters and thresholds in a timely manner, taking into consideration recent typologies in relation to fraudulent transactions and financial mule accounts, including new digital fraud techniques and modus operandi in other jurisdictions.				



Partnering with Zimperium: Your Step Towards Compliance and Security

Join hands with Zimperium to navigate the complexities of RMIT Malaysia regulation with ease and confidence. We can help create a more secure and trustworthy digital financial ecosystem for your customers.

Learn How Banking Institutions Are Leveraging MAPS

About Zimperium

Zimperium, the world leader in mobile security, protects over 1,500 global customers—including leading enterprises and governments—against the ever-evolving mobile threat landscape. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging AI-driven, autonomous security to counter evolving threats including mobile-targeted phishing (mishing), malware, app vulnerabilities and compromise, as well as zero day threats. As cybercriminals adopt a mobile-first attack strategy, Zimperium helps organizations stay ahead with proactive, unmatched protection of the mobile apps that run your business and the mobile devices relied upon by your employees. Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank.

www.zimperium.com

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244